

EXHIBIT 24



SECURITY & COMPLIANCE PROGRAM QUARTERLY OVERVIEW

AUGUST 16, 2019



SolarWinds Scorecard

NIST Maturity Level

Security Category	2017	2018	2019
Identify	0.8	2.0	3.0
Protect	1.5	3.0	3.2
Detect	1.0	2.8	3.6
Respond	0.8	2.8	3.6
Recover	0.7	2.0	2.0
Overall	1.0	2.5	3.1

Maturity Level	Description
0	There is no evidence of the organization meeting the security control objectives or is unassessed
1	The organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objectives
2	The organization has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance
3	The organization has a documented, detailed approach to meeting the security control objectives, and regularly measure its compliance
4	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations
5	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost effective manner

© 2019 SolarWinds Worldwide, LLC. All rights reserved.

@solarwinds



PROTECT

Highlights

- Access and privilege to critical systems / data is inappropriate. Need to improve internal processes | procedures
- Comprehensive firewall protection for Corporate IT and web properties (Palo Alto Next Gen firewalls in place (58) | Web Application Firewalls (WAF) on all key marketing properties)
- Improved end point protection. End user devices coverage: 80% SEP | 85% encryption | 95% DLP. IT servers coverage: 91% SEP. Hosted environment assessment WIP
- Moving towards Zero Trust model (where we loosely protect all and strongly protect those that can-do material harm). Less requirements on VPN
- Spam / Phishing still a challenge. Adversaries are getting better. Increase in whale phishing (55 million messages blocked 1H2019)
- Movement to make Azure AD authoritative source of identity. Plan to enable federation for all critical assets
- Additional monitoring via SOC is planned for 2nd half of the year



Security Category	Objective	NIST Maturity Level
Next Generation Firewalls	Palo Alto Firewalls are deployed and actively monitored across the company	5
Web Application Firewalls	WAFs are deployed for marketing properties but not for production products	3
Endpoint Protection and Encryption	Endpoint protection and encryption is deployed and actively managed across the company	4
Data Leakage Protection	Data leakage protection is deployed across the company and actively monitored	3
Spam / Phishing Detection / Response	Email protections are in place to monitor spam, detect phishing and deter known email scammers	3
Authentication, Authorization and Identity Management	User identity, authentication and authorization are in place and actively monitored across the company	1
Protect Maturity Level		3.2

CONFIDENTIAL – INTERNAL USE ONLY © 2019 SolarWinds Worldwide, LLC. All rights reserved.

@solarwinds



FINANCIAL: ENTERPRISE ACCESS MANAGEMENT (SOX COMPLIANCE)

Description

Access management describes the management of individual identities, their authentication, authorization, roles, and privileges within the enterprise in order to minimize security risks associated the use of privileged and non-privileged access.

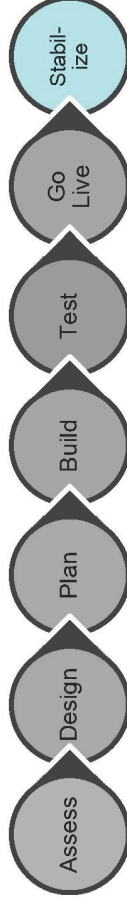
Scope:

- Enterprise information systems (CoreIT, MSP, Cloud)
- Privileged and non-privileged users
- On-premise & SaaS applications

KPIs



Timeline



Budget

Q1 18	Q2 18	Q3 18	Q4 18	TOTAL
\$0	\$0	\$0	\$0	\$0

Issues, Risks & Dependencies

Cat No.	Description	Action Required
I.1	Concept of least privilege not followed as a best practice	ID existing permission levels within the enterprise
I.2	Use of shared accounts throughout internal and external applications	Work with teams to decommission use of shared accounts
I.3	Project scope expanded to include SOX compliance requirements	Need to assess existing controls to ensure alignment with SOX requirements

Key Milestones / Status

Ph.	Milestone	Start	Finish	Status
1	Align access controls and permissions to security standards and guidelines	1/1/2018	4/20/2018	Complete
2	Map existing assessment of access controls to defined guidelines and standards.	2/1/2018	6/29/2018	Complete
3	Align / validate access controls with SOX compliance requirements. Outline MVP objectives	6/29/2018	7/31/2018	Complete
4	Identify extended team roles and responsibilities	7/1/2018	7/31/2018	Complete
5	Identify admins / approvers, define ABAC	7/1/2018	8/30/2018	Complete
6	Define standards, approval workflows, long term solution/recommendations/POC	8/1/2018	9/30/2018	Complete
7	Finalize Access SARF. Implement SARF changes / exceptions	12/2019	2/2019	Complete
8	Internal audit, Holtzman audit, Audit remediation	1/2019	2/2019	Audit in Progress